REMARKS

Claims 1-24 are pending in the present application. By this Amendment, at least claim 1 is amended to represent the present invention more clearly, and some of the previous claims have been cancelled.

Abstract:

The abstract stands object to due to minor informalities. However, the abstract has been amended to correct such minor informalities. Accordingly, withdrawal of this objection is respectfully requested.

Claim Objections:

Claims 1, 3, 6 and 15-17 stand objected to due to certain informalities. However, each of claims 1 and 15-17 has been amended to correct such informality. As such, withdrawal of this objection is respectfully requested.

35 U.S.C. §112, Second Paragraph Rejection:

Claims 1-24 stand rejected under 35 U.S.C. §112, second paragraph, for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

This rejection is respectfully traversed.

It is respectfully submitted that the specification and claims 1, 15-19, 23 and 24 have been amended to overcome this rejection. In addition, with regard to item 46, it is believed that the term “single photon or so” is definite. Accordingly, withdrawal of this rejection is respectfully requested.

As to the Merits:

As to the merits of this case, the Examiner maintains the following rejections:

1) claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Townsend (USP 5,675,648) in view of Werner et al. ("Eavesdropping using quantumnondemolition measurements");

2) claims 2, 5, 8-1 1, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Townsend in view of Werner et al. and further in view of Bethune et al. (USP 6,188,768);

3) claims 3-4 and 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bethune;

4) claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Townsend in view of Werner et al. in and further in view of Bartelt et al. (The Wigner Distribution Function-An Alternative Signal Representation in Optics);

5) claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Townsend in view of Werner et al. and further in view of Bethune et al. (US 6,188,768) and Lee USp 5,665,423);

6) claims 15-21 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bethune et al (US 6,188,768) in view of Mazourenko et al (US 6,272,224), herein referred to as Maz, in further view of Townsend (US 5,675,648); and

7) claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bethune et al. in view of Mazourenko et al. (USP 6,272,224) in further view of Townsend and Bartelt et al.

Before going into detailed discussions of each claims, Applicant respectfully emphasize the fundamental difference between the present quantum cipher communication and the other quantum cipher communication as described in Townsend et al. or Bethune et al.

In the latter conventional quantum cipher communication, a weak signal light is detected by a single photon detector. Commonly used device is an avalanche photodiode (APD) that is biased beyond reverse breakdown voltage (Townsend col. 4, 51-59). A single photon detector measures the number of photons, that takes a discrete value, i.e. 0,1,2, ... Specifically, for the case of an APD, what is measured is whether a single photon exists or does not exist. Therefore, it is easy to assign a bit value because the existence of a photon may correspond to a bit value 1.

For the case of the present invention, a weak signal light is detected by an optical balanced homodyne detector, in which a weak signal light is superimposed with an intense reference light on a beam splitter which has a transmittance and reflectance equal to each other, and the difference signal between two output from the beam splitter is amplified. The measured physical observable is a quadrature phase amplitude of the signal light. In principle, the amplitude takes a continuous value, i.e. a real number. In addition, due to the uncertainty principle of quantum mechanics, one cannot get a definite result; the measured value of the amplitude takes a random real number even for the same input state. This is the fluctuation of the quantum state. Although the measured value for each light pulse is random, the statistical frequency distribution is completely characterized by the input quantum state, as is shown in Fig.3 of the present invention. So, the physical observable is fundamentally different from the case of a single photon detector. In fact, in the conventional quantum cipher communication using a single photon detector, there is no such quantum fluctuation under an idealized situation. Furthermore, due to

the nonorthogonality of quantum states, the measured values of the amplitudes become the same for the different input state. Thus, even if the sender transmits two different quantum states each of which is assigned to bit value 0 or 1, respectively, the recipient may observe the same result. This property leads to the intrinsic error rate for the quantum cipher communication using an optical balanced homodyne detector.

Based upon the above observations, the present invention offers the method for assigning a bit value from a continuous real number, detecting an eavesdropper, controlling the error rate of the recipient, correcting the phase difference developed by reason of an external cause, measuring the winger distribution of the quantum state while doing quantum cipher communication, and so on.

In the following, each of the rejections is respectfully traversed.

Independent Claim 1:

Claim 1 calls using *a phase difference between a weak signal light which is so weak that a change in its quantum mechanical state is detectable and an intense reference light for communicating a privacy key, wherein said phase difference is produced by a sender and a recipient adding a phase on the signal light or the reference light; it has an optical homodyne detector which detects said phase difference as a difference signal of the detector, wherein said*

phase difference is determined by comparing said difference signal with threshold values which is determined from a quantum-mechanical probability distribution of said difference signals which are determined from a quantum-mechanical probability distribution of said difference signals obtained from a set of said phase differences assigned bit 0 or bit 1; and wherein an eavesdropping is detected by a change in said quantum-mechanical probability distribution of said difference signals, which is produced by the eavesdropping operation.

The present invention discloses in the original specification from line 32 of page 15 to line 21 of page 16 with the attached figures Figs. 3A to 3D that "*a quantum-mechanical probability distributions_of said difference signals obtained from a set of said phase differences assigned bit 0 or bit 1 using an optical balanced homodyne detector*". And Fig.4a illustrates the typical measurement result. The balanced homodyne detector can measure *the quantum-mechanical probability distribution*, because it measures a quadrature-phase amplitude of the electro-magnetic field and the measurement of a quadrature-phase amplitude yields probability distribution determined by the law of quantum mechanics.

On the other hand, Townsend (5,675,648) discloses in col. 3 at line 37 -45 that "It can be seen from the photon transmission probabilities shown in FIG.1 that if the total phase shift $\Delta\varphi$(that is the transmitter phase shift minus the receiver phase shift) is an integer multiple of π radians the photon will behave deterministically, and will be detected at one or the other of the

interferometer output ports depending on the value Δ φ." From these descriptions, it is apparent that the system of Townsend can only distinguish the phase shift (difference) as 0 or π, because it measures the phase difference detecting by which port of the interferometer the photon is detected and the ports exists only two corresponding to the 0 and the π, and that it can not measure *a quantum-mechanical probability distribution*, because the photon having a phase difference minutely differed from 0 or π depended on quantum-mechanical fluctuation are deterministically detected as either of 0 or π.

The present invention discloses in the original specification from line 22 of page 16 to line 14 of page 17 that "*said phase difference is determined by comparing said difference signal with threshold values which are determined from a quantum-mechanical probability distribution of said difference signals obtained from a set of said phase differences assigned bit 0 or bit 1*". On the other hand, it is apparent that Townsend does not disclose or teach the above limitation of the present invention, because the system of Townsend can not measure the quantum-mechanical probability distribution as mentioned above.

The present invention discloses in the original specification from line 5 to line 21 of page 22 that "*an eavesdropping is detected by a change in said quantum-mechanical probability distribution of said difference signals, which is produced by the eavesdropping operation*". It is apparent that Townsend does not disclose or teach the above limitation of the present invention,

because the system of Townsend can not measure the quantum-mechanical probability distribution as mentioned above.

The Examiner argues in the page 10 of Office Action regarding claim 1 that Townsend discloses that "2. Wherein an eavesdropping is detected by the recipient measuring a change in a quantum-mechanical probability distributions of said difference signal, which is produced by the eavesdropping operation (col 3, lines 56-64).

However in the col 3, lines 56-64 of Townsend, it is described that "After completion of the quantum communication, the receiver and transmitter test for the presence of an eavesdropper by using the public channel to compare which photons were encoded and decoded using the same type of phase shift, but not the results of the individual measurements (i.e. whether a 0 or a 1 was obtained). The procedure is completed by comparing the actual measured bits for a random subset of this data in order to test for any eavesdropper–induced errors".

From these descriptions, it is apparent that in the system of Townsend, a detection of eavesdropping is done by comparing the actual measured bits for a random subset of this data (which means specifically that the receiver and transmitter announce the value of the aimed bit whether it is 0 or 1 by using the public channel), and by calculating the ratio of the number of bits not coincided with each other to the number of the total test bits.

On the other hand, in the system of the present invention, a detection of eavesdropping is done at the recipient side only by *detecting a change of the quantum-mechanical probability distribution of the difference signals obtained from a set of the phase differences assigned bit 0 or bit 1.*

Therefore the above description of Townsend does never mean that the detection of Townsend is equal to that of the present invention, namely to detecting *a change of the quantum-mechanical probability distribution of the difference signals*. This is more apparent from the reason above mentioned that the system of Townsend can not measure the quantum-mechanical probability distribution.

In the col 3, lines 50-56 of Townsend, it is described that "This effect of the quantum uncertain principle is the basis of the security of the system, since any eavesdropper will be forced to make random choices of which measurement type to use. This procedure will inevitably lead to some incorrect choices which in turn lead the eavesdropper to sometimes send on wrong type of bit to the receiver, thus causing a detectable error rate."

The above description is the same of the description at page 21 lines 8-19 of the present specification, but methods of eavesdropping are not limited to the above method that an eavesdropper measures a signal and resends the signal, also there exists the method described at

page 22 lines 5-8 of the present specification that an eavesdropper takes the step to isolate and measure a portion of a signal light to acquire the information and to amplify a resultant loss of the signal light. In the case of this eavesdropping, the method of Townsend can not detect it as described at page 22 lines 8-9 of the present specification, but the method of the present invention using *a change of quantum-mechanical probability distribution of said difference signals* can detect it as described at page 22 lines 9-21 of the present specification. Therefore, the present invention has an inventive step.

The Examiner argues in the page 10 of Office Action regarding claim 1 that "Townsend does not disclose "it has an optical balanced homodyne detector which detects said phase difference as a difference signal of the detector, wherein the phase difference is determined by comparing said difference signal with a threshold value." However, the examiner submits that the limitation is well known in the art. Further, the limitation is disclosed by Werner (p640, Figure 1a) ".

However, it is described in the currently amended claim1 that the threshold values which are determined from a quantum-mechanical probability distribution of said difference signals obtained from a set of said phase differences assigned bit 0 or bit 1. Therefore, it is no longer a limitation well known in the art.

In addition, since present invention uses *a weak signal light which is so weak that a change in its quantum mechanical state is detectable and an intense reference light*, it is possible to amplify a quantum state of the weak signal light by the intense reference light by homodyne detection. On the other hand, the system of Townsend can not amplify a quantum state of a signal photon by a reference signal, because it uses a single photon detector and not a balanced homodyne detector. The feature of the present invention to be able to amplify a quantum state of signal is very useful in practical use, which is never disclosed in Townsend.

In Werner at page 640 and Fig.1, a method of eavesdropping by using an optical balanced homodyne detector and the configuration of the detector for eavesdropping operation are disclosed. In the description, it is described that one of the arm of the detector consists of Kerr effect medium, when a signal photon sent by the sender for quantum cryptography exists in the arm, then a phase of the local light of the detector in the arm is affected by the electric field of the signal photon due to the Kerr effect, the phase affected is detected by the detector, and therefore an eavesdropping is possible. These descriptions would disclose that an optical balanced homodyne detector can detect a phase of photon very sensitively. But it is apparent that detecting a phase of photon sensitively can not disclose the limitation of the present invention that using a phase difference--- for communicating a privacy key, ---an optical homodyne detector which detects said phase difference as a difference signal of the detector, that phase difference is determined by comparing said difference signal with the threshold values which are

predetermined from a quantum-mechanical probability distribution of said difference signals obtained from a set of said phase differences assigned bit 0 or bit 1, and that an eavesdropping is detected by a change in said quantum-mechanical probability distribution of said difference signals, which is produced by the eavesdropping operation.

In view of the above, it is respectfully submitted that Townsend and Werner completely fail to disclose or suggest the limitations of the present invention.

In addition, while claim 2 has been cancelled, Bethune is also related to the present invention, therefore the differences between Bethune and the present invention are explained as follows.

In Bethune on column 2, lines 51-57, it is described that "The key information is decoded at a detection stage at the sender that uses two detectors, one of which detects a first polarization state corresponding to the phase difference between the two phase shifts being 0 and the other of which detects a second polarization state corresponding to the phase difference between the two phase shifts being π". And further, in Bethune on column 6 line 64 to column 7, line 11, it is described that the polarization state having a phase difference even multiple of $\pi/2$ is directed to the signal detector D0 (Fig.2), and the other polarization state having a phase difference odd multiple of $\pi/2$ is directed to the signal detector D1(Fig.2). From these descriptions, it is

apparent that the system of Bethune can only distinguish the phase shift (difference) as 0 or π, because it measures the phase difference detecting by which detector the photon is detected and the detector exists only two corresponding to the 0 and the π. It can never measure a quantum-mechanical probability distribution of the quadrature-phase amplitude, because Bethune uses a single photon detector (col.2, line 14,or col.7, line 30) and not a balanced homodyne detector.

If supposing to accomplish to measure a quantum-mechanical probability distribution of the phase differences in the system of Bethune, the system needs a large number of optical paths, each of which can be chosen by a photon according to its polarization state minutely differed from 0 or π depended on quantum-mechanical fluctuation, and each end of which has a detector for detecting whether a photon comes here or not, and to measure a frequency distribution of photon-detections against these optical paths. However these configurations are never disclosed or suggested in Bethune, therefore the limitations of the present invention never meet to Bethune.

In addition, Bethune describes on Col.2, line33 that "the return pulses from the receiver are attenuated to single–photon pulses" From this description, it is apparent that the signal photons and the reference photons are both very weak, on the contrary to the present invention wherein a signal light is so weak that a change in its quantum mechanical state is detectable and a reference light is intense. Therefore, the system of Bethune is different from the system of the present invention.

In view of the above, it is respectfully submitted that it is apparently not possible to make the present invention by combining Bethune with the teachings of Townsend and Werner.

Independent Claim 15:

The Examiner argues in the page 22 of Office Action regarding claim 15 that "b. An amplifying means for amplifying a difference signal between said electric signals (col.6, lines 1-5 and 20-28).

In Bethune on col.6, lines 1-5, it is described that "Also shown at the second channel end is a power meter monitor 28 for detecting how much light is received at the second channel end. The power meter monitor 28 can be used to detect if an eavesdropper is probing the system with pulses", and in the Fig.2 of Bethune, the amplifying means 28 is shown. But it is apparent that the amplifying means 28 of Bethune is only used for amplifying a total power of the optical path, for detecting a power increase of the optical path by eavesdropping operation, on the contrary to the present invention that uses amplifying means for amplifying a difference signal between the electric signals converted by a pair of photoconductive diodes from two output lights which are generated by a superimposing means, as described by the limitation that "*a pair of photoconductive diodes for converting two output lights from said superimposing means into respective electric signals; and an amplifying means for amplifying a difference signal between*

said electric signals". Therefore it is apparent that the amplifying means of Bethune is quite differ from that of the present invention in the function of implementation.

In Bethune on col.6, lines 20-28, it is described that "Because each of the pair of pulses has traveled precisely the same distance from PBS1 to the Faraday mirror 22 and back to PBS1, the return pulse RP1 and the return pulse RP2, which has passed through delay stage 18, will recombine at PBS1 into a single return signal designated RS. Signal RS will have a polarization state that is determined by the difference of the phase shifts imparted to P2 and RP1 by PM2 and PM1, respectively, prior to their recombination at PBS1". This description means that the phase shifts imparted by the sender and the receiver is used for generating the polarization state of RS signal, which determines to which optical path RS signal is lead. However, in this paragraph there is no description about the amplifying means of Bethune.

The Examiner argues in the page 22 of Office Action regarding claim 15 that "Maz discloses the recipient apparatus comprises of a superimposing means for superimposing said signal light and said reference light, either of which is phase changed by said modulation means of the recipient's apparatus (Fig 4 and col 4, lines 1-14). Maz further discloses the recipient apparatus comprises a pair of photo-detector for converting two output lights into respective electric signals (col. 3, lines 19-24).

In Maz on column 2, lines 51-57, and Fig 4 describes and shows a superimposing means for signal light and reference light such as a semi-transparent blade122. But in Maz, only one of the two outputs of the semi-transparent blade122 is used for combining the signal light and reference light into a common optical path, on the contrary to the present invention that uses two light outputs of the superimposing means as indicated in Fig.1 of the present invention, the one of which is lead to photoconductive diode 7a and the other of which is lead to photoconductive diode 7b, then it becomes possible to detect a phase difference added by sender and recipient as a difference signal of the two photoconductive diode outputs amplified. In Fig 4 of Maz, one of the output of the semi-transparent blade122 is ignored, which is directing to downward in the figure, because the output is not necessary for the system of Maz. Therefore Maz does not disclose the limitation of the present invention that "*for converting two output lights from said superimposing means into respective electric signals*".

In Maz on column 3, lines 19-24, and Fig 2 describes and shows that "a pair of photo-detector for converting two output lights into respective electric signals". But on column 3, lines 17-18, it is described that "At the output from the interferometer there are two photon detectors 61, 62 and a decryption and counting circuit 64". From this description, it is apparent that the pair of photo-detector of Maz are used for photon counting which detects the phase difference as either of 0 or π detecting by which detector of 61, 62 a photon is detected, as in Townsend and Bethune. Therefore, Maz uses the photo-detectors for the photon counting, and does not use for

converting the two output lights from the superimposing means into respective electric signals which have continuous values depending on the amplitudes of the two output lights, as described in the limitation of the present invention that "*photoconductive diodes for converting two output lights from said superimposing means into respective electric signals; and an amplifying means for amplifying a difference signal between said electric signals*".

Moreover, since the claim 15 is currently amended as dependent on claim1, Maz also does not disclose the limitations of the claim 1 of the present invention.

In view of the aforementioned amendments and accompanying remarks, Applicant submits that that the claims, as herein amended, are in condition for allowance. Applicant requests such action at an early date.

If the Examiner believes that this application is not now in condition for allowance, the Examiner is requested to contact Applicant's undersigned attorney to arrange for an interview to expedite the disposition of this case.

If this paper is not timely filed, Applicant respectfully petitions for an appropriate extension of time. The fees for such an extension or any other fees that may be due with respect to this paper may be charged to Deposit Account No. 50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP

Thomas E. Brown
Attorney for Applicant
Registration No. 44,450
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

TEB/jl